UNIVERSITY OF SOUTHAMPTON

Applying Gamification to Teaching Cyber Security

By

Reece Buckle

Project Supervisor: Dr Nawfal Fadhel

Second Examiner: TBA

A project progress report submitted for the award of BSc Computer Science

Department of Electronics and Computer Science

Novemeber 2020

Abstract

To write near the end / later on

Statement of Originality

- I have read and understood the ECS Academic Integrity information and the University's Academic Integrity Guidance for Students.
- I am aware that failure to act in accordance with the Regulations Governing Academic Integrity may lead to the imposition of penalties which, for the most serious cases, may include termination of programme.
- I consent to the University copying and distributing any or all of my work in any form and using third parties (who may be based outside the EU/EEA) to verify whether my work contains plagiarised material, and for quality assurance purposes.

You must change the statements in the boxes if you do not agree with them.

We expect you to acknowledge all sources of information (e.g. ideas, algorithms, data) using citations. You must also put quotation marks around any sections of text that you have copied without paraphrasing. If any figures or tables have been taken or modified from another source, you must explain this in the caption and cite the original source.

I have acknowledged all sources, and identified any content taken from elsewhere.

If you have used any code (e.g. open-source code), reference designs, or similar resources that have been produced by anyone else, you must list them in the box below. In the report, you must explain what was used and how it relates to the work you have done.

I have not used any resources produced by anyone else.

You can consult with module teaching staff/demonstrators, but you should not show anyone else your work (this includes uploading your work to publicly-accessible repositories e.g. Github, unless expressly permitted by the module leader), or help them to do theirs. For individual assignments, we expect you to work on your own. For group assignments, we expect that you work only with your allocated group. You must get permission in writing from the module teaching staff before you seek outside assistance, e.g. a proofreading service, and declare it here.

I did all the work myself, or with my allocated group, and have not helped anyone else.

We expect that you have not fabricated, modified or distorted any data, evidence, references, experimental results, or other material used or presented in the report. You must clearly describe your experiments and how the results were obtained, and include all data, source code and/or designs (either in the report, or submitted as a separate file) so that your results could be reproduced.

The material in the report is genuine, and I have included all my data/code/designs.

We expect that you have not previously submitted any part of this work for another assessment. You must get permission in writing from the module teaching staff before re-using any of your previously submitted work for this assessment.

I have not submitted any part of this work for another assessment.

If your work involved research/studies (including surveys) on human participants, their cells or data, or on animals, you must have been granted ethical approval before the work was carried out, and any experiments must have followed these requirements. You must give details of this in the report, and list the ethical approval reference number(s) in the box below.

My work did not involve human participants, their cells or data, or animals.

ECS Statement of Originality Template, updated August 2018, Alex Weddell aiofficer@ecs.soton.ac.uk

Contents

1 Introduction

1.1 Problem Summary

Problem Statement

Despite the existence of many cyber security awareness programs, there is still a lack of effective, widespread cyber security training

As modern day technology is ever evolving, the number of users who interact with technology on a daily basis increases consequently. As a result, the risk of an individual, or business, begin targeted by cyber-crime increases proportionately. In particular, small and medium-sized businesses (SMBs) are the biggest sectors which are hit hardest by cyber-crime (Bada, Maria & Nurse, 2019), which stem from a variety of problems including budget restraints or simply because they simply do not understand the changing dynamic and importance of cyber security.

In fact, as a consequence of COVID-19 changing the dynamic of industry standards this year, a statistical analysis of all cyber-crimes targeting individuals has increased by an average of 43% May 2020 that is in comparison with May 2019 Buil-Gil et al. (2020). Furthermore, this new trend in targeted hacking of individuals, which has increased by 77.41% Buil-Gil et al. (2020)), has arisen from the fact that employees are encouraged to work from home via their personal computers. This new dynamic has fed into a new strategy whereby cyber-criminals are moving laterally into organisational infrastructure by targeting and infecting employees at their less secure personal computers Lallie et al. (2020).

In regards to this problem, it is clear that most cyber attacks are successful due to social engineering and human error and, although many government schemes, compliance regulations and training material exist to tackle this, there now presents a gap in the industry where all working adults need sustainable training from home. Furthermore, it has also been shown that game-based learning can have a strong impact on the learning outcomes of cyber security in comparison to similar tutorials or training material (Tioh, Mina & Jacobson, 2017) as well as the fact that game-designers are typically experts in motivating their intended target audience. Therefore, this project will aim to address the problem of an individual falling victim to cyber-crime by creating a serious game.

In order to measure the effectiveness of my serious game, this paper presents the following research question and hypothesis:

Research Question

Does teaching cyber security through a gamified medium improve user confidence in protecting against cyber attacks?

Hypothesis

Creating a wide-reachable, easy to access cyber security game will leave users feeling more confident in protecting themselves against cyber attacks.

1.2 Goals

The goal of this project is to investigate how to effectively apply gamification mechanics in order to teach cyber security principles in an effective, and sustainable way. To date, this report includes a critical evaluation of pre-existing 'serious' cyber security games as well as research into literature that heavily explores current trends in cyber security training and mechanics for game-based learning. The expected final result of this project is to create a an online web application comprised of small training mini-games and game-based mechanics to facilitate learning in a continuous and sustainable way.

1.3 Scope

The main web application should be freely accessible to all users with an internet connection and, if time permits, multi-platform such that it can be accessed via mobile devices and tablets as well. As identified in (Forde (2020), this project will incorporate a variety of core game mechanics including:

- Avatar / User Profile
- Badges / Privileges
- Challenge
- Competition
- Collaboration
- Feedback / Guidance
- Goals / Objectives
- Incentives / Rewards
- Leaderboards
- Points System
- Progress / Levels
- Role Playing
- Story
- Tips / Hints System

2 Literature Review & Research

A report on the background research and literature search

2.1 The Problem with Current Cyber Security Training Programs

This report will specifically look at non-required training schemes which deliver material comparable to those of delivered through gamified means and teaching.

Bada & Nurse (2019) appropriately identifies a number of problems with current training programs that are designed for SMBs. These include:

- SMEs can be heavily constrained by a limited budget
- SMEs can be difficult to reach as they do not understand the severity of data breaches
- SMEs can be distracted heavily distracted by the operational costs and time - requirement for setting up and running their small business
- SMEs struggle to identify their assets in terms of risk

To summarise these points, cyber security training programs need to be cost effective and target the specific needs and requirements of the targeted business. These needs / requirements are often identified via a risk assessment.

Both Bada & Nurse (2019) and Aldawood & Skinner (2019) agree that providing generalised security advice / training alone (from an independent advisor) is not very effective for changing the behaviour of upper management/employees for a SMBs. For example, traditional training methods are generally undertaken in a formal serious environment whereby the generality of the information leads to a situation of recipients not absorbing the information well. The reasons for this stem from the fact that because they may not see how it relates to their workplace, it is simply not relevant to them. This generalisation also causes a lack of in depth/conceptual understanding for 'multi-faceted social engineerning attacks'

2.2 Difficulties that Pre-Existing Cyber Security Games Face

As identified in my research of pre-existing cyber security games (see Appendix A), many of the serious games and simulations I reviewed relied heavily on presenting facts and then subsequently quizzing the player. The problem with this approach however is that most people can use common sense to rule out incorrect answers which fails to invoke critical thinking in a way that would keep the player sufficiently engaged.Roepke & Schroeder (2019) emphasises the importance of diversifying learning strategies of a serious game by incorporating a variety of

factual, conceptual and procedural teaching methodologies.

For conceptual learning, rather than simply quiz the player on their ability to perform fact recall, the game should instead explore basic concepts in a stimulating way - i.e why it is extremely important to use strong passwords, or even better, 2 factor authentication and randomly generated passwords!

For procedural learning, both Nova Cyber Lab and Classcraft tackle this very well by starting off with simple challenges and progressively increasing the difficulty and complexity as time goes on. To further elaborate, Nova Cyber Land provides a series of minigame challenges which increase in difficulty and complexity. classcraft is exemplary because, as a gamified management system, it encourages players within a team to continually expand upon their knowledge - working towards new goals and objectives collaboratively as the school term progresses.

To summarise, both of these are extremely important because of the rapidly changing landscape of cyber security. Cite: roepke2019problem also argues that cybercriminals will always be engineering new attack vectors so it is imperative for people to adapt their way of thinking when interacting with technology - this is one field where cynicism pays off.

Finally, roepke2019problem also identifies through their comprehensive case study that a lot of games are designed primarily for university students (as part of a research project or module delivery) and corporations but do not have much availability in the public domain. In fact, my through my own research (albeit a much smaller sample size) also correlates this where another point I identified is that any publicly available cyber security game I could find, was considerably outdated especially by today's game development engines and tools available for creating light weight games within web applications!

2.3 Why Use a Game-Based Learning Approach?

Because it's fun! As Bada & Nurse (2019), frequently explores the main issues with educating SMEs/SMBs can often result because not only do these SMEs have a lack of understanding of the importance , this audience can be particularly hard to reach due to business owners and employees being overwhelmed with the management of such a small business. Being able to teach smart and safety awareness here and there is still a win regardless of how big it is!

Furthermore, if done right there is consistent evidence that game-based learning can be much more effective in comparison to equivalent traditional training methods and schemes. Although there isn't much long term conclusive studies on the effectiveness of 'serious' cyber security games, Tioh et al. (2017) explores several small case studies which did conclude that serious games can have a stronger

impact on the learning outcomes on their subjects. However, a problem with this methodology in general is hard to measure since long - term memory and behavioural change cannot be easily measured, especially when it varies a lot depending on the individual's personality traits. There is also the question of which group these serious games are targeting and the purpose for their existence - a serious game aiming to educate the public in general about avoiding common engineered cyber attacks such as phishing sites and emails can be very different to a specific targeted cyber security compliance/training course targeted for employees who need to acknowledge strict networking security! It is very reasonable to assume that simple games are just not appropriate to enforce these regulations.

Aldawood & Skinner (2019) also emphasises the need to make training methods as entertaining as possible as traditional methods can often result in becoming a tedious task in which the employee is often asked to do within working hours and desires to complete as fast as possible to resume normal work. This often causes the person to absentmindedly progress through these training materials and not absorb the material in a constructive way

Some key strengths to game based learning - as identified by Tioh et al. (2017), include:

- Rapid progress paired with instant feedback
- Excel in player engagement which is important for keeping the user motivated
- Allow the player to learn from mistakes in a safe. Non punishing environment
- Serve as a platform to encourage self-learning at the user's desired pace
- Allow player to become deeply immersed into the 'game - world' where learning feels like a secondary objective and having fun is the primary - especially if the game is done right (such as hacknet - on steam)
- Relatively cheap and low cost to produce and distribute among multiple platforms to target multiple audiences of people - more serious games should be given as "fun" homework in schools, or as secondary learning objectives in businesses

2.4 A Brief Analysis of Pre-Existing Educational Cyber Security Games

My methodology for reviewing cyber security games was two fold: at first came with a simple google search using keywords including: 'cyber', 'security', 'serious games', 'gamification', 'game-based learning', 'training which mostly returned games aimed for kids and students. Building on from this, I then searched reports

via google scholar and ieee explore (soton library guides) looking for the same keywords, but specifically articles, books and journals evaluated serious cyber security games. I then iteratively went through cyber security games reviewed in these papers and searched for them via google. Most of these results returned training approaches aimed, as a service, for businesses and employees. These games which I could not physically play or review I searched for game play demonstrations via their company website / youtube and used this as a basis for my review.

In particular, I concluded 4 different categories of serious game based teaching which could be applied to teaching cyber security. It is also worth noting most of these games were web applications

- Web applications - Mini games (with simple point and click interactivity)
- Training Simulations
- Multiplatform
- Task management e.g. Classcraft

It is also worth noting the abundance of web applications over multi-platform (android/ios apps) is likely due to the easier development time and accessibility for this platform.

Some benefits of task management classcraft is really nice at sustaining cyber security learning / interactivity which a key point expressed by Roepke & Schroeder (2019).
Also the benefits of development point-and-click web applications are accessibility and short development time, however its reasonable to assume the impact of these products is a lot less in comparison to how gamification principles are applied in classcraft

Training simulations can be very effective for cooprotations in particular, however outside of these typical office type careers their relevance quickly diminishes, and they're often nowhere near as fun as the other variations of game-based learning. It then raises the important question if it is even worthwhile to attempt to gamify these simulations when it might be more appropriate to target these companies specifically with the cyber security knowledge/security standards/schemes they're required to understand. The exception to this is the multiplatform game of threats which uses ipads/big screens in a business environment to separate employees into attackers and defenders and undergo these simulations in real time - really promoting constructive feedback and guidance. Therefore Singleplayer simulations = bad. multiplayer/cooperative simulations = good.

2.5 A Review of Riskio

2.6 A Review of Ashell's Gamification Toolkit

3 The Proposed Final Design

3.1 Title of Game Idea Here

Write about initial/final idea here and attached game design template

3.2 A Justification of this Approach

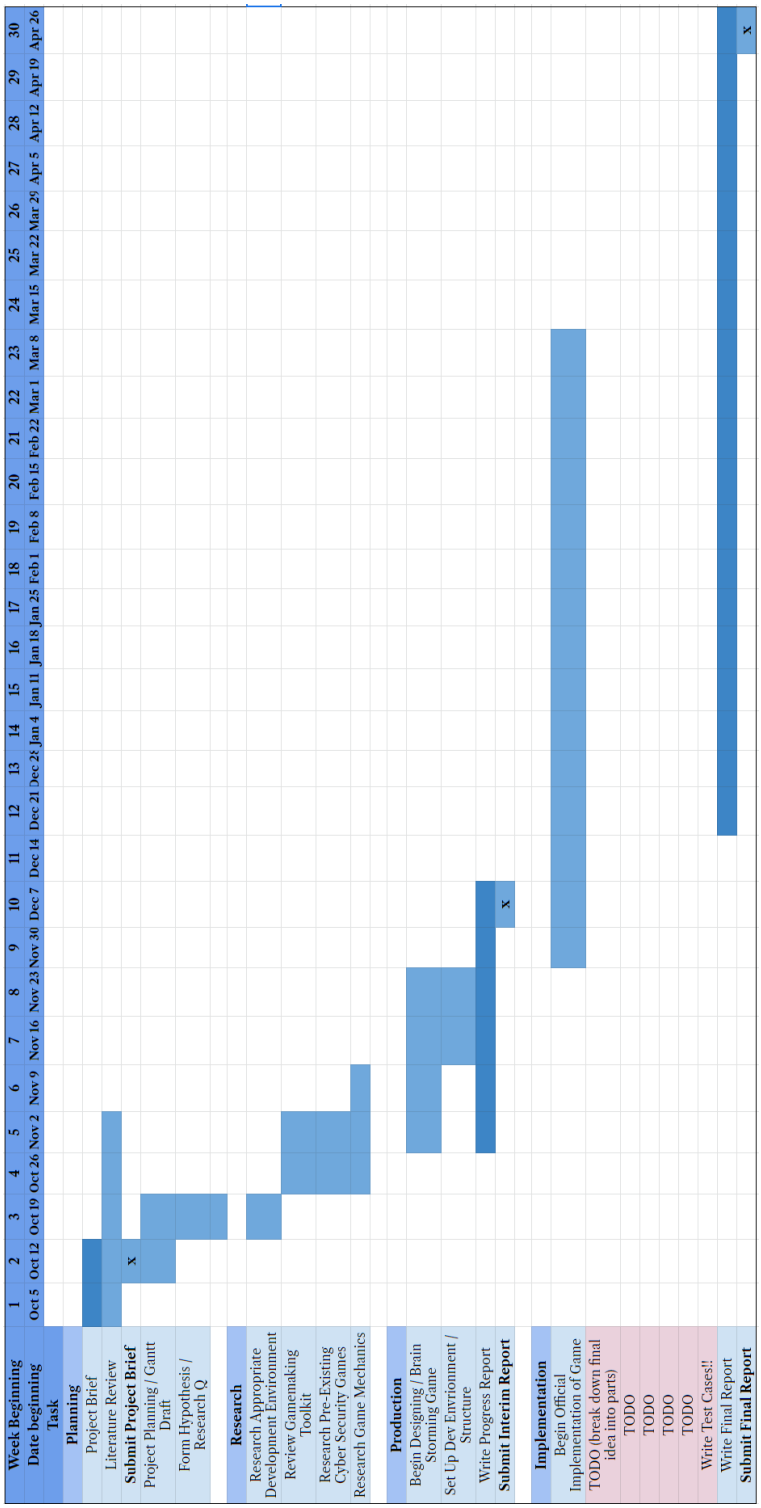
3.3 An Account of the Work to Date

4 Future Work

4.1 Remaining Work

Plans for second half/winter term

4.2 Gantt Chart Illustrating Progress & Goals



4.3 Risk Assessment

Risk	Probability (1 - 5)	Severity (1 - 10)	Risk Exposure (E = P × S)	Mitigation
Project deadlines not being met	4	10	40	By starting early and establishing soft deadlines as Milestones. Also by meeting with project supervisor weekly, I can contiuously receive an evaluation of my progress
Mental health impacts due to Covid19 / final undergraduate year stress	3	8	24	Hard to fully bullet proof this one, but currently following a healthy and balanced routine at home and doing my best to stay ahead of all coursework deadlines. Should things get too difficult, will seek help from University services before the problem gets too big. Also will communicate any issues I have with my project supervisor at any time
Over/under estimating scope of implementation	3	7	21	By constructing my project modularly (in the form of minigames) that I can aim to develop more/less dynamically as the year progresses. By not having one large game, I can guarantee a functional level of completeness across my final implementation
Relevant cyber security principles are not effectively taught	3	7	21	By identifying the most appropriate methodologies/content to target with a serious cyber security game through thorough literature review and frequently evaluating my project through peer-reviewed feedback
Final project doesn't answer original problem statement/hypothesis and is not relevent for research	2	8	16	By continuously referring back to my initial problem statement and hypothesis with thorough literature review undertaken before the development of my implementation. This will help to ensure my final project is both relevant and appropriate
Gamified mechanics are not appropriately utilised	2	7	14	By identifying a list of tools and mechanics through thorough literature review which is fundamentally important to the design aspects of my game.
Loss of work/data from: PC breaking or cloud storage servers going down	1	10	10	By storing the contents of my work across multiple platforms (Southampton Git, Locally on my PC and also within Google Drive / One Drive). This should account for any one of those services halting or breaking.
Stolen work/data from: cloud storage account being hacked or falling victim to ransomware	1	10	10	By using a combination of strong randomally generated passwords and 2-Factor authentification on all cloud storage platforms (e.g. Google Drive). Also manually backing up important files weekly on a secondary harddrive protected by an airgap

5 Bibliography

Aldawood, H. & Skinner, G. (2019), 'Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues', *Future Internet* **11**(3), 73.

Bada, M. & Nurse, J. R. (2019), 'Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (smes)', *Information & Computer Security* .

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S. & Díaz-Castaño, N. (2020), 'Cybercrime and shifts in opportunities during covid-19: a preliminary analysis in the uk', *European Societies* pp. 1–13.

Forde, A. T. (2020), 'A gamification toolkit for improving cyber security standards adoption', *Computers & Security* .

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C. & Bellekens, X. (2020), 'Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic', *arXiv preprint arXiv:2006.11929* .

Roepke, R. & Schroeder, U. (2019), The problem with teaching defence against the dark arts: A review of game-based learning applications and serious games for cyber security education., *in* 'CSEDU (2)', pp. 58–66.

Tioh, J.-N., Mina, M. & Jacobson, D. W. (2017), Cyber security training a survey of serious games in cyber security, *in* '2017 IEEE Frontiers in Education Conference (FIE)', IEEE, pp. 1–5.

6 Appendix

6.1 Appendix A - A Review of Cyber Security / Serious Games

Game	Cyberland - Cyber Security Challenge
Game Type	Web Application Point and Click
Target Audience	Children, Teenagers, Students (High school - University level)
Description	Cyber Security Challenge UK is an organisation which hosts a variety of mini games (Cyberland), competitions and networking between schools, universities, businesses and government institutes
Key Teachings / Findings	Examples of minigames which teach: - Identifying phishing emails - Command line simulator - Firewall simulator (analyse incoming network activity and grant/deny requests - Database simulator -(remove old accounts, sanitise personal information, check admin clearance) - Coffee shop network simulator (using unprotected networks vs VPN and shoulder surfing) - IoT home simulator - making sure all IoT devices have latest software update - Courthouse simulator - demonstrating cyber security laws and ethics - Cipher cracking simulator - Password strength making game - Data leak mystery solver - Malware simulator (demonstrates different types of malware/ransomware and they work)
Mechanics Identified	• Competition • Feedback / Guidance • Tips / Hints • Story • Goals / Objectives

Game	Cyberland - Cyber Security Challenge
Game Type	Web Application Point and Click
Target Audience	Children, Teenagers, Students (High school - University level)
Description	Cyber Security Challenge UK is an organisation which hosts a variety of mini games (Cyberland), competitions and networking between schools, universities, businesses and government institutes
Key Teachings / Findings	Examples of minigames which teach: - Identifying phishing emails - Command line simulator - Firewall simulator (analyse incoming network activity and grant/deny requests - Database simulator -(remove old accounts, sanitise personal information, check admin clearance) - Coffee shop network simulator (using unprotected networks vs VPN and shoulder surfing) - IoT home simulator - making sure all IoT devices have latest software update - Courthouse simulator - demonstrating cyber security laws and ethics - Cipher cracking simulator - Password strength making game - Data leak mystery solver - Malware simulator (demonstrates different types of malware/ransomware and they work)
Mechanics Identified	• Competition • Feedback / Guidance • Tips / Hints • Story • Goals / Objectives

Game	Game of Threats
Game Type	Multiplatform - (Mobile, Tablet, PC), Multiplayer
Target Audience	Businesses - Employees
Description	Employees are split into teams of attackers and defenders who work together to simulate scenarios of cyber attacks and appropriate responses
Key Teachings / Findings	- Teaches people about cyber security trends and to understand the consequences of cyber attacks and what you can do to mitigate the impacts - Helps people understand the mindset of both attackers and defenders- - Prompts discussion with colleagues in teams to popularise cyber security readiness
Mechanics Identified	● Feedback / Guidance ● Incentives / Rewards ● Competition

Game	Webonauts Internet Academy
Game Type	Web Application Point and Click Side Scroller
Target Audience	Children (aged 7-12)
Description	Puts the player as an astronaut in which they can rank up their status by demonstrating smart and good behaviour
Key Teachings / Findings	Teaches children: - How to be respectful online - How to protect themselves online - Looking for trustful website certificates - Establishing privacy settings on profile - Not giving out and using weak passwords
Mechanics Identified	● Avatar ● Feedback / Guidance ● Tips / Hints ● Badges / Privileges

Game	Targeted Attack
Game Type	Web Application Point and Click
Target Audience	Businesses - Employees
Description	Targeted Attack places you as a CEO in a simulation of business growth and defence from cyber attacks
Key Teachings / Findings	Teaches employees: - Smart and safe decision making - Threat level of different types of cyber attacks and how to mitigate them
Mechanics Identified	● Feedback / Guidance ● Story ● Challenge

Game	Classcraft
Game Type	Web Application, Point and Click, Multiplayer, Productivity - Management
Target Audience	School Students
Description	Classcraft incorporates gamifiication principles through the use of management software to set goals and challenges within a classroom and encourages teamwork between students
Key Teachings / Findings	Teaches employees: - Smart and safe decision making - Threat level of different types of cyber attacks and how to mitigate them
Mechanics Identified	● Avatar ● Leaderboard ● Competition ● Badges / Privileges, ● Feedback / Guidance ● Goals / Objectives ● Incentive / Rewards ● Point Systems

Game	Cyber- security Lab
Game Type	Web Application Point and Click
Target Audience	Businesses - Employees
Description	Allows the player to choose a business they'd like to start and require them to spend defence points in different areas of cyber defence
Key Teachings / Findings	Teaches children via minigames: - how to spot phishing emails - how to construct strong passwords - Simple programming principles
Mechanics Identified	● Avatar ● Achievements ● Progress / Levels ● Point System ● Tips / Hints ● Feedback / Guidance

Game	Keep Tradition Secure
Game Type	Web Application Point and Click
Target Audience	University Students
Description	You are a campus student trying to take down a fictional cyber criminal by making smart cyber security decisions
Key Teachings / Findings	Teaches students: - Smart decision making on campus (using public networks vs campus VPN) - Quiz based - Gives out prizes for student participants
Mechanics Identified	● Tips / Hints ● Feedback / Guidance ● Rewards / Incentives

Game	Hacknet
Game Type	Downloadable, Single Player, Point and Click
Target Audience	Gamers
Description	Hacknet is a paid game (on Steam) which is a terminal-based hacking simulator
Key Teachings / Findings	Teaches player: - How to navigate networks - Search for hidden files/folders - Authorisation bypass - Heavy use of terminal/linux commands in a tutorial environment
Mechanics Identified	● Story ● Progress / Levels ● Feedback / Guidance ● Steam Achievements

Game	Cyber Awareness Challenge
Game Type	Downloadable Training Simulator
Target Audience	Businesses Employees
Description	Single Player simulation of everyday life within the workplace and how to behave safely and responsibly
Key Teachings / Findings	- Teaches employees how to be safe in the workplace - Gives points for correct answers and guidance for both right and wrong answers
Mechanics Identified	● Tips / Hints ● Feedback / Guidance ● Story ● Points System